INSTRUCTIONS FOR ON-LINE CE BRIEF

TO VIEW THE BRIEF, CLICK ANYWHERE ON THIS PAGE. YOU CAN THEN USE THE FOLLOWING KEYS TO NAVIGATE THROUGH THE BRIEF:

RIGHT ARROW KEY (FORWARD)
LEFT ARROW KEY (BACK)
PAGE UP/DOWN KEYS

HEADQUARTERS UNITED STATES MARINE CORPS

- ANNUAL REFRESHER TRAINING
- ANTITERRORISM/FORCE PROTECTION
- COUNTER-ESPIONAGE

SECURITY PROGRAMS AND INFORMATION MANAGEMENT

ANNUAL REFRESHER TRAINING

SECURITY PROGRAMS AND INFORMATION MANAGEMENT BRANCH

BRANCH HEAD	MR. OLIVER	614-2320/3609
DEPUTY/COMSEC	MR. SIMMS	614-2305/2154
SECURITY OFF	MAJ HAUGHTON	614-2320/3609
OPS CHIEF	MSGT HOPEWELL	614-2320/3609
PHYSICAL SECURITY	SGT HANSMANN	614-2305/2154

STAFF AGENCY SECURITY MANAGERS

DMCS	MAJ VANZANDBERGEN/GYSGT RIVERA
AR	GS-12 COLLIER/MSGT GRESHAM
ARIE	CAPT RICHARDS/MSGT WITHERSPOON
AVN	CAPT BURCKART/SSGT POMRINK
C4	CAPT ROBINSON/SSGT ROBERTSON JR
CMC	LCDR GALVIN/MGYSGT DUNNUCK
CL	CAPT GROHARING/SGT GAROFOLA
HD	LTCOL WEBER/SSGT WAYNE
HQBN	CAPT AUSTIN/MSGT JACKSON
HS	CAPT ZAMBITO/HM1 DANDO
I	GS-15 SILVER/GYSGT SINCLAIR
I&L	SGT ROMERO/SGT SALAS

STAFF AGENCY SECURITY MANAGERS

IG	CW04 MILLER/GYSGT THOMASCHAMBERS
JA	GS-15 RUTIGLIANO/GYSGT ALGER
OLA	CWO3 BEAUCHAMP/MSGT JENKINS
PA	CAPT FISHER/CAPT MCSWEENEY
PP&O	SES-2 GEOFFROY/GYSGT ARCAUTE
P&R	CAPT KOCH/GYSGT TULL
REL	CAPT KLOAK/RPC DRAKE
SD	GS-11 PAIGE/CDR SYRING
SPD	CAPT PAIGE/CAPT CINCOTTA

PROTECTION OF CLASSIFIED INFORMATION

- ALL DOD PERSONNEL, MILITARY AND CIVILIAN OCCUPY A POSITION OF TRUST AND ARE EXPECTED TO SAFEGUARD CLASSIFIED NATIONAL SECURITY INFORMATION

- INDIVIDUALS WHO RECEIVE CLASSIFIED INFORMATION ARE REQUIRED TO HAVE:

  - APPROPRIATE CLEARANCE ELIGIBILITY
  - APPROVED ACCESS
  - NEED TO KNOW

- JUST BECAUSE YOU HAVE A CLEARANCE, DOES NOT MEAN YOU HAVE ACCESS

LEVELS OF CLASSIFICATION

- TOP SECRET
  - EXCEPTIONAL GRAVE DAMAGE TO NATIONAL SECURITY
  - SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)
- SECRET
  - SERIOUS DAMAGE TO NATIONAL SECURITY
  - NATIONAL AGENCY CHECK WITH LOCAL AGENCY CHECK AND CREDIT CHECK (NACLAC)
- CONFIDENTIAL
  - DAMAGE TO NATIONAL SECURITY
  - NATIONAL AGENCY CHECK WITH LOCAL AGENCY CHECK AND CREDIT CHECK (NACLC)
  - ACCESS NATIONAL AGENCY CHECK WITH WRITTEN INQUIRIES (ANACI)

PERIODIC REINVESTIGATIONS

- IF YOU HAVE ACCESS TO CLASSIFIED MATERIAL AND YOUR LAST INVESTIGATION IS OVER THE ESTABLISHED TIME FRAME, YOU NEED TO BE REINVESTIGATED

  - TOP SECRET/TOP SECRET (SCI) EVERY 5 YEARS
  - SECRET EVERY 10 YEARS
  - CONFIDENTIAL EVERY 15 YEARS

- A PERSON MAY NOT HAVE ACCESS TO CLASSIFIED INFORMATION WITHOUT AN UP-TO-DATE INVESTIGATION

CONTINUOUS EVALUATION PROGRAM

- THE PROCESS BY WHICH ALL INDIVIDUALS, (MARINES, CIVILIAN MARINES, AND CONTRACTORS), WHO HAVE SECURITY CLEARANCE ELIGIBILITY ARE MONITORED TO ENSURE THEY CONTINUE TO MEET THE LOYALTY, RELIABILITY AND TRUSTWORTHINESS STANDARDS EXPECTED OF INDIVIDUALS WHO HAVE ACCESS TO CLASSIFIED INFORMATION

CONTINUOUS EVALUATION

- THE CONTINUOUS EVALUATION PROGRAM RELIES ON ALL PERSONNEL WITHIN THE COMMAND TO REPORT QUESTIONABLE OR UNFAVORABLE INFORMATION WHICH MAY BE RELEVANT TO A SECURITY CLEARANCE DETERMINATION

- INDIVIDUALS ARE ENCOURAGED TO REPORT TO THEIR SUPERVISOR OR APPROPRIATE SECURITY OFFICIAL AND SEEK ASSISTANCE FOR ANY INCIDENT OR SITUATION WHICH COULD AFFECT THEIR CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

- CO-WORKERS HAVE AN OBLIGATION TO ADVISE THEIR SUPERVISOR OR APPROPRIATE SECURITY OFFICIAL WHEN THEY BECOME AWARE OF INFORMATION WITH POTENTIAL SECURITY CLEARANCE SIGNIFICANCE

- THE GOAL IS EARLY DETECTION OF AN INDIVIDUAL'S PROBLEMS. SUPERVISORS ARE IN A UNIQUE POSITION TO RECOGNIZE PROBLEMS EARLY AND MUST REACT APPROPRIATELY TO ENSURE BALANCE IS MAINTAINED REGARDING THE INDIVIDUAL'S NEEDS AND NATIONAL SECURITY REQUIREMENTS

13 CONTINUOUS EVALUATION CATEGORIES

- INVOLVEMENT IN ACTIVITIES WHICH, OR SYMPATHETIC ASSOCIATION WITH PERSONS WHO, UNLAWFULLY PRACTICE OR ADVOCATE THE OVERTHROW OR ALTERATION OF THE UNITED STATES GOVERNMENT BY UNCONSTITUTIONAL MEANS
- FOREIGN INFLUENCE CONCERNS/ASSOCIATION WITH FOREIGN NATIONALS OR NATIONS
- DUAL CITIZENSHIP
- SEXUAL BEHAVIOR THAT IS CRIMINAL OR REFLECTS A LACK OF JUDGMENT OR DISCRETION
- QUESTIONABLE JUDGMENT, UNTRUSTWORTHINESS, UNRELIABILITY OR UNWILLINGNESS TO COMPLY WITH RULES AND REGULATIONS TO COOPERATE WITH SECURITY CLEARANCE PROCESSING

13 CONTINUOUS EVALUATION CATEGORIES (CONT'D)

- UNEXPLAINED AFFLUENCE OR EXCESSIVE INDEBTEDNESS
- ALCOHOL ABUSE
- ILLEGAL OR IMPROPER DRUG USE/INVOLVEMENT
- APPARENT MENTAL, EMOTIONAL OR PERSONALITY DISORDER(S)
- CRIMINAL CONDUCT
- NONCOMPLIANCE WITH SECURITY REQUIREMENTS
- ENGAGEMENT IN OUTSIDE ACTIVITIES WHICH COULD CAUSE A CONFLICT OF INTEREST
- MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

FINANCIAL CONCERNS

- Financial concerns is the number one reason for the Department of the Navy Central Adjudication Facility to issue a letter of intent to deny/revoke a security clearance.
- An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds.
- Individuals with financial issues should seek the assistance of a debt counselor.
- It is recommended that individuals with financial concerns take a look at their credit reports prior to submitting their EPSQ.
- Failure to list delinquent debts on your EPSQ may adversely affect your clearance eligibility.
- Early intervention is the best course of action if you are experiencing financial problems.

HANDLING CLASSIFIED INFORMATION

- ALWAYS USE A COVER SHEET

- CLASSIFIED MAIL-OUTS GO THROUGH THE HQMC CLASSIFIED MATERIAL CONTROL CENTER (CMCC ROOM 2107)

- WHEN TRANSPORTING CLASSIFIED MATERIAL TO OTHER LOCATIONS
  - COURIER CARD IS REQUIRED
  - DOCUMENT MUST BE DOUBLE WRAPPED(PROTECTED)

- WORKING PAPERS MUST BE ACCOUNTED FOR AFTER 180 DAYS FROM DATE OF CREATION

- CLASSIFIED MATERIAL PICK-UPS ARE CONDUCTED DAILY AT THE CMCC

- UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION/ MATERIAL IS PUNISHABLE IN FEDERAL COURT AND UNDER THE UNIFORM CODE OF MILITARY JUSTICE

TOP SECRET CONTROL

- All Top Secret Material must have a HQMC barcode and be reported to the HQMC Top Secret Control Officer via the Staff Agency Top Secret Control Officer.
- With the exception of NATO material, Secret material and below are not entered into the HQMC classified inventory.
- A record of disclosure must be maintained for each top secret document.
- Each individual that views or handles a top secret document must sign the record of disclosure.

NATO INFORMATION

- The USMC SIPRNET is authorized for NATO transmission up to NATO Secret.
- When sending e-mail it is the senders responsibility to ensure that the receiver is cleared for NATO and has a need to know.
- A listing of accredited enclaves is posted on the Central U.S. Registry (www.cusr.army.mil).
- NATO Secret an above material are controlled and must be entered in the HQMC NATO inventory when printed or downloaded to media.
- All equipment that stores and or processes NATO Secret information must be registered with the HQMC NATO Control Officer and be marked appropriately.

CLASSIFIED BRIEFS

- GOVERNMENT FACILITIES APPROVED FOR THE CONDUCT OF CLASSIFED BRIEFINGS (FACILITIES SUCH AS HOTELS ARE NO LONGER APPROVED)

- CLEAR ALL ATTENDEES

- DEVELOP BRIEFS ON CLASSIFIED PCs

- ENSURE THE SECURITY OF BRIEFING ROOM

- PRIOR TO CONDUCTING CLASSIFIED BRIEFS TO FOREIGN NATIONALS, COORDINATE WITH DEPUTY COMMANDANT INTEL DEPARTMENT(IOC)

COMMUNICATIONS SECURITY

- DISCUSSION OF CLASSIFIED INFORMATION OVER UNSECURED TELEPHONE LINES OR IN THE PRESENCE OF UNCLEARED PERSONNEL IS A SECURITY COMPROMISE

- ONLY NSA APPROVED DEVICES (STU/STE TELEPHONES) ARE AUTHORIZED FOR THE DISCUSSION OF CLASSIFIED MATERIAL AND THEN ONLY IN THE SECURE MODES OF OPERATION. BE AWARE OF UNCLEARED PERSONNEL IN ADJACENT LOCATIONS

- THE NIPRNET IS NOT CERTIFIED FOR THE TRANSMISSION OF CLASSIFIED MATERIAL. ONLY CLASSIFIED NETWORKS ARE APPROVED FOR THE DISSEMINATION OF CLASSIFIED MATERIAL

COMPROMISE OF CLASSIFIED INFORMATION

- REPORT ALL COMPROMISES OR SUSPECTED COMPROMISES TO THE HQMC SECURITY OFFICER VIA YOUR AGENCY SECURITY MANAGER
- PRELIMINARY INQUIRY WILL BE CONDUCTED TO DETERMINE THE FACTS SURROUNDING A POSSIBLE LOSS OR COMPROMISE
- IF NECESSARY, JAGMAN INVESTIGATION WILL BE CONDUCTED TO PROVIDE MORE DETAILED INFORMATION AND RECOMMEND CORRECTIVE ACTION AND/OR DISCIPLINARY ACTION

SPILLAGES

- The most common security incident at HQMC over the last couple years is the introduction of classified material on the NIPRNET (spillage).
- Spillages should be reported immediately.
- Delay in reporting spillages could result in the classified material replicating on multiple servers and is very expensive and time consuming to clean-up.
- When a spillage occurs, contact your ISC and your Agency Security Manager immediately.

ADMINISTRATIVE PROCEDURES

- ALL PERSONNEL ARE REQUIRED TO CHECK IN WITH YOUR AGENCY SECURITY MANAGER PRIOR TO CHECKING IN WITH THE HEADQUARTERS MARINE CORPS (HQMC) SECURITY MANAGER

- UPON DETACHMENT FROM HEADQUARTERS MARINE CORPS (HQMC) YOU NO LONGER HAVE A NEED-TO-KNOW (MARINES, CIVILIAN MARINES AND CONTRACTORS)

  - MAINTAIN CLEARANCE ELIGIBILITY
  - LOSES ACCESS FOR CLASSIFIED MATERIAL
  - NEW COMMAND MAY GRANT ACCESS

- CHECK OUT WITH AGENCY SECURITY MANAGER (DEBRIEF)

- CHECK OUT WITH HQMC SECURITY MANAGER (DEBRIEF AND BADGE RETURN)

- CHECK OUT WITH THE SSO (SCI ACCESS)

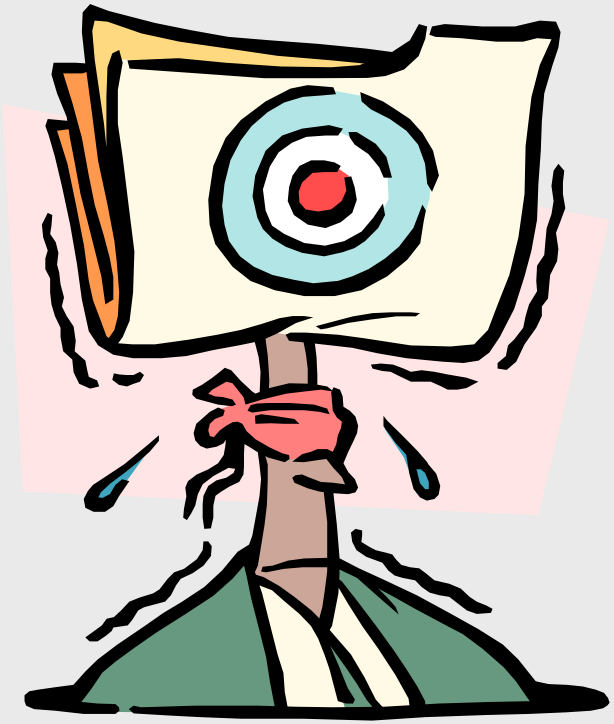
REFERENCES

- FOR ADDITIONAL INFORMATION REFER TO:

- SECNAVINST 5510.30A – DEPARTMENT OF THE NAVY PERSONNEL SECURITY PROGRAM

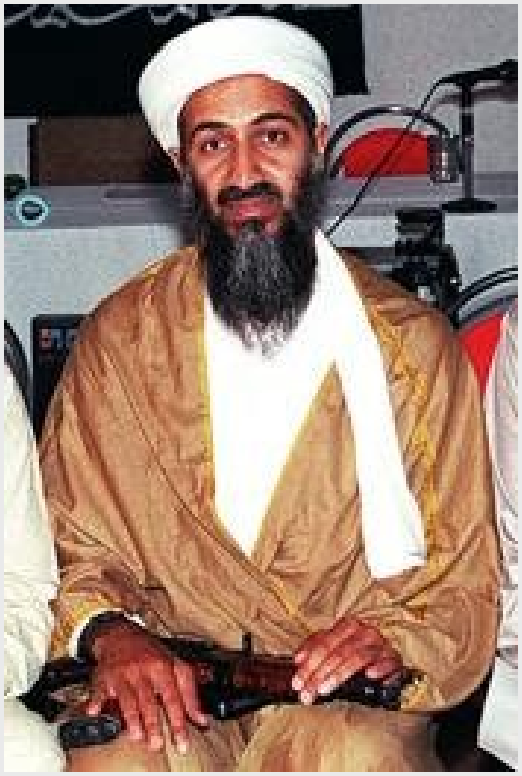
- SECNAVINST 5510.36 – DEPARTMENT OF THE NAVY (DON) INFORMATION SECURITY PROGRAM (ISP) REGULATION

ANTITERRORISM/PERSONAL PROTECTION BRIEFING



TERRORISM

THE CALCULATED USE OF VIOLENCE OR THREAT OF VIOLENCE TO GENERATE FEAR, INTENDED TO COERCE OR TO INTIMIDATE GOVERNMENTS OR SOCIETIES IN THE PURSUIT OF GOALS THAT ARE GENERALLY POLITICAL, RELIGIOUS OR IDEOLOGICAL



ANTITERRORISM

- DEFENSIVE MEASURES USED TO REDUCE THE VULNERABILITY OF INDIVIDUALS AND PROPERTY TO TERRORIST ACTS, TO INCLUDE LIMITED RESPONSE AND CONTAINMENT BY LOCAL MILITARY FORCES

- THE DOD COMBATING TERRORISM PROGRAM DEALS WITH ANTITERRORISM AND SEEKS TO REDUCE THE LIKELIHOOD THAT DOD PERSONNEL, FACILITIES AND MATERIAL WILL BE ATTACKED, AND TO MITIGATE THE EFFECTS OF SUCH ATTACKS SHOULD THEY OCCUR

FORCE PROTECTION CONDITIONS

NORMAL - EXISTS WHEN THERE IS NO KNOWN THREAT

ALPHA - EXISTS WHEN THERE IS A GENERAL THREAT OF POSSIBLE TERRORIST ACTIVITY AGAINST PERSONNEL AND INSTALLATIONS

BRAVO - EXISTS WHEN AN INCREASED AND MORE PREDICTABLE THREAT OF TERRORIST ACTIVITY EXISTS

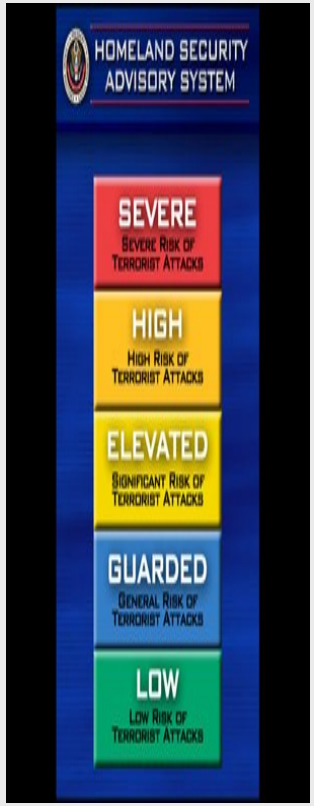
CHARLIE - EXISTS WHEN AN INCIDENT OCCURS OR WHEN INTELLIGENCE IS RECEIVED INDICATING THAT SOME FORM OF TERRORIST ACTION IS IMMINENT

DELTA - EXISTS WHEN A TERRORIST ATTACK HAS OCCURRED, OR WHEN INTELLIGENCE INDICATES THAT A TERRORIST ACTION AGAINST A SPECIFIC LOCATION IS LIKELY

HOMELAND SECURITY ADVISORY SYSTEM (HSAS)

PROVIDES A COMPREHENSIVE AND EFFECTIVE MEANS TO DISSEMINATE INFORMATION REGARDING THE RISK OF TERRORIST ATTACKS TO FEDERAL, STATE, AND LOCAL AUTHORITIES AND TO THE AMERICAN PEOPLE

THREAT CONDITIONS CHARACTERIZE THE RISK OF TERRORIST ATTACK. THE HSAS ESTABLISHES FIVE THREAT CONDITIONS



HOMELAND SECURITY ADVISORY SYSTEM CONTINUED

LOW CONDITION - GREEN
- LOW RISK OF TERRORIST ATTACKS

GUARDED CONDITION - BLUE
- GENERAL RISK OF TERRORIST ATTACKS

ELEVATED CONDITION - YELLOW
- SIGNIFICANT RISK OF TERRORIST ATTACKS

HIGH CONDITION – ORANGE
- HIGH RISK OF TERRORIST ATTACKS

SEVERE CONDITION - RED
- SEVERE RISK OF TERRORIST ATTACKS

TERRORIST ATTACKS

- TERRORISTS HAVE USED VARIOUS TYPES OF ATTACKS TO FURTHER THEIR GOALS.

- MOST COMMON ARE AS FOLLOWS:
  - BOMBING
  - ASSASSINATION
  - ARMED RAIDS
  - HOSTAGE-TAKING
  - KIDNAPPING
  - SKYJACKING

- MOST TERRORIST ACTIONS OCCUR SUDDENLY, LEAVING LIMITED OPPORTUNITY TO REACT AND TAKE DEFENSIVE MEASURES

FORCE PROTECTION

FORCE PROTECTION CONSISTS OF ACTIVE AND PASSIVE MEASURES DESIGNED TO DETER AND DEFEAT THREATS DIRECTED TOWARD MILITARY SERVICE MEMBERS, DOD CIVILIANS, THEIR FAMILIES, AND THE FACILITIES AND EQUIPMENT NECESSARY FOR THE EXECUTION OF DOD OPERATIONS

BEFORE TRAVEL

- IT IS IMPORTANT TO REMAIN ALERT AT ALL TIMES DURING HEIGHTENED FORCE PROTECTION CONDITIONS OR WHILE YOU ARE IN A HIGH THREAT ENVIRONMENT

  - LEARN SOMETHING ABOUT YOUR DESTINATION (HTTP://TRAVEL.STATE.GOV)

  - WHAT IS THE CURRENT POLITICAL CLIMATE (HTTP://TRAVEL.STATE.GOV)

  - IS THERE ANY OFFICIAL INFORMATION AVAILABLE CONCERNING THE THREAT LEVEL (HQMC FOREIGN TRAVEL BRIEF, CURRENT WORLDWIDE THREAT ALERT, OR HTTP://TRAVEL.STATE.GOV)

  - READ YOUR LOCAL NEWSPAPER OR NATIONAL NEWS MAGAZINES FOR CURRENT EVENTS COVERAGE OF THE REGION

FAMILY TRAINING

- ALL FAMILY MEMBERS SHOULD TRY TO LEARN ABOUT THE CUSTOMS, CULTURE, HISTORY AND GEOGRAPHY OF THE AREA TO WHICH THE DOD MEMBER HAS BEEN ASSIGNED (HTTP://TRAVEL.STATE.GOV, FOREIGN TRAVEL BRIEF, OR CJCS GUIDE 5260: A SELF-HELP GUIDE TO ANTITERRORISM)
  - THIS SHOULD INCLUDE LEARNING AT LEAST A FEW PHRASES IN THE COUNTRY'S LANGUAGE FOR USE IN EMERGENCIES
  - KNOW HOW TO ASK FOR THE POLICE OR MEDICAL CARE
  - CONSIDER CARRYING SMALL CARDS WITH EMERGENCY PHRASES ON THEM. YOU MAY EVEN CONSIDER MAKING CARDS WITH PICTURES OR INTERNATIONAL SYMBOLS SO YOU CAN POINT OUT TO COMMUNICATE YOUR NEEDS

FAMILY SECURITY MEASURES

- "CHECKING IN" WITH FRIENDS AND FAMILY TO LET THEM KNOW WHEN AND WHERE YOU ARE GOING AND WHEN TO EXPECT YOU BACK

- LEARNING HOW TO USE THE LOCAL TELEPHONE SYSTEM AND MEMORIZING EMERGENCY NUMBERS

- KNOWING THE LOCATIONS OF POLICE, FIRE STATIONS, THE U.S EMBASSY OR ANY OTHER SAFE, PUBLIC PLACE WHERE REFUGE OR ASSISTANCE MAY BE FOUND

- DEVELOPING AND PRACTICING EMERGENCY PROCEDURES FOR USE IN THE HOME (SUCH AS EVACUATION PROCEDURES)

- NEVER ADMITTING STRANGERS TO THE HOME WITHOUT PROPER IDENTIFICATION

FAMILY OPERATIONAL SECURITY

- DON'T PUT YOUR NAME ON THE MAILBOX OR EXTERIOR WALLS OF YOUR RESIDENCE

- DON'T ANSWER THE PHONE WITH YOUR NAME AND RANK

- TEACH CHILDREN NOT TO GIVE OUT FAMILY INFORMATION TO STRANGERS ON THE PHONE

- CONSIDER THE USE OF AN UNLISTED PHONE NUMBER

- DESTROY ALL TRASH THAT COULD BECOME A SOURCE OF INFORMATION

- TEACH CHILDREN TO BE ON GUARD AGAINST ANY APPROACH OR QUESTIONING BY STRANGERS

- ADVISE SCHOOL OFFICIALS THAT CHILDREN ARE NOT TO BE RELEASED TO STRANGERS UNDER ANY CIRCUMSTANCES

HARD TARGET

- BECOME A HARD TARGET

- A HARD TARGET CONSISTS OF:

- INACCESSIBLE
  - CAREFUL ABOUT DIVULGING PERSONAL INFORMATION ABOUT YOURSELF OR FAMILY MEMBERS

- OBSERVANT
  - PAY ATTENTION, OBSERVE DETAILS, TRY TO NOTICE THINGS GOING ON AROUND YOU

- AWARE
  - COMPREHEND WHAT YOU OBSERVE AND TAKE APPROPRIATE ACTION. DEVELOP A “SIXTH SENSE” FOR DETECTING POTENTIALLY DANGEROUS SITUATIONS

HARD TARGET-CONTINUED

- MAKE CHANGES TO VARY YOUR ROUTINE. CHANGE YOUR ROUTE TO AND FROM WORK AND VARY YOUR DEPARTURE AND ARRIVAL TIMES. CHANGE THE TIMES AND PLACES FOR YOUR DAILY EXERCISE

- MAINTAIN A LOW PROFILE

  - DRESS AND BEHAVE IN PUBLIC IN A MANNER THAT “BLENDS IN” WITH LOCAL CUSTOMS

  - AVOID CLOTHING THAT MAKES YOU STAND OUT AS A FOREIGNER

  - BE SENSITIVE TO THE COUNTRIES CUSTOMS; FOR EXAMPLE, IN SOME COUNTRIES A PUBLIC DISPLAY OF AFFECTION IS INAPPROPRIATE

SAFETY IN VEHICLES

- KEEP YOUR VEHICLE IN GOOD SHAPE
- KEEP YOUR GAS TANK AT LEAST HALF FULL
  - LOCK YOUR GAS TANK
  - PARK IN SECURE AREAS WHEN POSSIBLE AND DO A WALK-AROUND INSPECTION OF YOUR VEHICLE BEFORE GETTING IN THE VEHICLE

DRIVING AWARENESS

- WHEN DRIVING, BE ALERT FOR ANY ATTEMPTS BY OTHERS TO STOP YOUR VEHICLE, BOX YOU IN, OR OTHERWISE RESTRICT YOUR MOVEMENT

- HAVE AN EVASION PLAN READY

- SOMETIMES MAKING A SIMPLE U-TURN IS ENOUGH TO GET YOU OUT OF DANGER

- PLOYS THAT HAVE BEEN USED IN THE PAST INCLUDE:

  - “BOXING” THE VICTIM IN AT STOP SIGNS AND LIGHTS
  - STAGING AN AUTO ACCIDENT IN YOUR PATH, OR HITTING YOUR VEHICLE FROM THE REAR OR SIDE
  - A BICYCLIST OR MOTORBIKE DRIVER “FALLS DOWN” IN YOUR PATH
  - USE OF VEHICLE ROADBLOCKS, CONES OR OTHER BARRIERS

SECURITY IN AIRPORTS

- WHEN FLYING TO/FROM A FOREIGN AIRPORT, CHECK IN QUICKLY AND PROCEED THROUGH PASSENGER SCREENING TO MORE SECURE AREAS

- AVOID THE PUBLIC ACCESS AREAS

- BE ALERT FOR PEOPLE BEHAVING SUSPICIOUSLY IN THE WAITING AREAS

- DON’T LET YOUR CARRY-ON LUGGAGE OUT OF YOUR SIGHT, AND DON’T AGREE TO “WATCH” SOMEONE ELSE’S LUGGAGE

- TRAVEL IN CONSERVATIVE CIVILIAN CLOTHING AND REMOVE ALL STICKERS AND BUSINESS CARDS FROM YOUR LUGGAGE

ON THE PLANE

- WHEN POSSIBLE, GET SEATING NEXT TO A WINDOW

- HIJACKERS GENERALLY SELECT PASSENGERS FOR ABUSE THAT ARE SITTING IN MORE EASILY ACCESSIBLE AISLE SEATS

  - SELECT A HIDING PLACE ON THE AIRCRAFT IN CASE YOU HAVE TO “DITCH” OFFICIAL DOCUMENTS, MILITARY ID OR YOUR OFFICIAL PASSPORT IN THE EVENT OF A HIJACKING

  - IF CONFRONTED DIRECTLY, DON’T LIE ABOUT YOUR DOD AFFILIATION

BAGGAGE CLAIM

- WHEN YOU ARRIVE AT YOUR DESTINATION:

- OBSERVE THE BAGGAGE CLAIM AREA FROM A DISTANCE
- WAIT FOR THE CROWD TO THIN OUT BEFORE CLAIMING YOUR LUGGAGE
- TRY TO STAY ON THE EDGE OF THE CROWD AS YOU PROCEED TO THE CUSTOMS LINES

HOTEL SECURITY

- WHENEVER POSSIBLE, STAY AT DOD FACILITIES

- IF YOU MUST STAY AT A HOTEL, PRACTICE THE FOLLOWING PRECAUTIONS:

  - AVOID TAKING A STREET-LEVEL ROOM

  - NOTE THE ESCAPE ROUTES AVAILABLE AND TRY THEM (YOU'LL FIND OUT IF DOORS ARE LOCKED/BLOCKED)

  - WHEN YOU ARE OUT OF YOUR ROOM, LEAVE THE LIGHTS AND RADIO OR TV ON

  - UNEXPECTED MAIL LEFT FOR YOU AT THE DESK OR SLIPPED UNDER YOUR DOOR SHOULD BE VIEWED WITH SUSPICION

HOTEL SECURITY CONTINUED

- CHECK THE HALLWAY BEFORE LEAVING AN ELEVATOR (OR YOUR ROOM), LOOK FOR PEOPLE LOITERING OR OBJECTS THAT ARE UNUSUAL OR OUT-OF-PLACE

- IF THE HOTEL IS EVACUATED DUE TO A BOMB THREAT, STAY OUT OF THE PARKING LOT AND GET A SAFE DISTANCE AWAY FROM THE BUILDING

HOSTAGE SITUATIONS

- IF, DESPITE YOUR PRECAUTIONS, YOU FIND YOURSELF HELD HOSTAGE:

- MAKE MENTAL NOTES OF DETAILS SUCH AS TIME IN TRANSIT, NOISES AND OTHER FACTORS THAT MAY HELP YOU IDENTIFY WHERE YOU ARE BEING TAKEN

- NOTE THE NUMBER OF CAPTORS, THEIR NAMES, PHYSICAL CHARACTERISTICS, ACCENTS, PERSONAL HABITS AND RANK STRUCTURE

- ATTEMPT TO CONVEY A SENSE OF YOUR PERSONAL DIGNITY. (YOU MAY DISCUSS NON-SUBSTANTIVE TOPICS SUCH AS SPORTS. THE GOAL IS TO BECOME A PERSON TO THE HOSTAGE TAKERS, RATHER THAN AN OBJECT.)

- MAKE EVERY EFFORT TO AVOID EMBARRASSING THE U.S. AND THE HOST GOVERNMENT

- LISTEN ACTIVELY TO THE TERRORISTS' FEELINGS ABOUT THEIR CAUSE, BUT NEVER PANDER, PRAISE, PARTICIPATE OR DEBATE

HOSTAGE RESCUE

- EPISODES OF KIDNAPPING AND HOSTAGE-TAKING OFTEN END WITH NO LOSS OF LIFE OR PHYSICAL INJURY TO THE HOSTAGE. IN THE EVENT OF A RESCUE, THE HOSTAGE AND THE RESCUE FORCE ARE IN EXTREME DANGER

- PROTECT YOURSELF BY FOLLOWING THESE RULES:

  - DO NOT RUN OR RESIST
  - DROP TO THE FLOOR AND REMAIN STILL
  - IF THAT IS NOT POSSIBLE, CROSS YOUR ARMS ON YOUR CHEST, BOW YOUR HEAD AND STAND STILL
  - WAIT FOR AND OBEY ALL INSTRUCTIONS
  - YOU MAY EVEN BE HANDCUFFED AND SEARCHED
  - THE RESCUE TEAM HAS TO IDENTIFY AND SORT OUT THE TERRORISTS, WHO MAY BE DISGUISED AS HOSTAGES

REPORTING

- BECOME AN ACTIVE PART OF FORCE PROTECTION

- IF YOU OBSERVE OR SUSPECT SUSPICIOUS ACTIVITY OR TERRORIST SURVEILLANCE OF YOU, YOUR COMMAND OR YOUR FAMILY, REPORT IT TO YOUR SUPERVISOR, SECURITY OFFICER OR POLICE

- IF OVERSEAS. CONTACT THE LOCAL CONSULATE OR EMBASSY PROVIDED IN YOUR FOREIGN TRAVEL BRIEF

REFERENCES

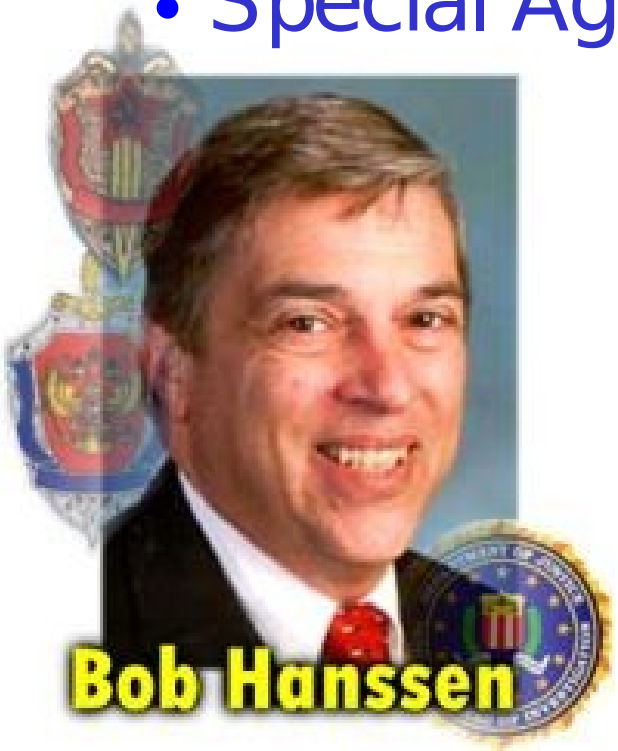
- FOR ADDITIONAL INFORMATION REFER TO:

- **CJCS GUIDE 5260: A SELF-HELP GUIDE TO ANTITERRORISM**
- **HTTP://WHITEHOUSE.GOV/HOMELAND/**
- **HTTP://TRAVEL.STATE.GOV/**

COUNTER-ESPIONAGE AWARENESS BRIEFING

2001: Just a Few Spy Bad Guys

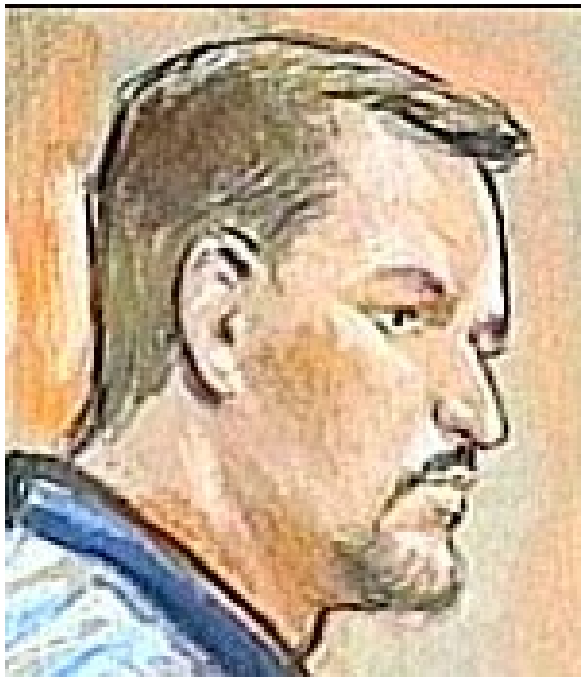
- Special Agent Robert Hansen, FBI



Espionage is occurring right now!

2001: Just a Few Spy Bad Guys

- Master Sgt Brian P. Regan, USAF (Ret)



Espionage is occurring right now!

2001: Just a Few Spy Bad Guys

- Col George Trofimoff, USAR (Ret)

Espionage is occurring right now!

2001: Just a Few Spy Bad Guys

(and Girls)

- Analyst Ana Belen Montes, DIA
- Multiple Arrests for Economic Espionage

Espionage is occurring right now!

WHAT IS COUNTERINTELLIGENCE?

Information gathered and activities conducted to protect against espionage, other intelligence activities, or sabotage conducted for or on the behalf of foreign powers, organizations or persons, or international terrorist activities

- Does not include Personnel, Physical, Document, and Communications Security programs

WHAT IS ESPIONAGE?

THE ACT OF OBTAINING, DELIVERING, TRANSMITTING, COMMUNICATING, OR RECEIVING INFORMATION ABOUT THE NATIONAL DEFENSE WITH AN INTENT, OR REASON TO BELIEVE, THAT THE INFORMATION MAY BE USED TO THE INJURY OF THE UNITED STATES OR TO THE ADVANTAGE OF ANY FOREIGN NATION

(JOINT PUB 1-02)

"The enemy's spies…must be sought out, tempted with bribes…and comfortably housed. It is through (their) information that we are able to acquire and employ local inward spies."

Sun Tsu

Who Can Pose a Threat?

- Foreign Governments
  - -- Traditional Adversaries
  - -- Economic Competitors
  - -- Foreign Intelligence and Security Services (FISS)
- Foreign Companies
- Terrorists and Narco-traffickers

“To lack intelligence is to be in the ring blindfolded.”

General David M. Shoup

Commandant USMC/1960-1963

What Do Our Adversaries Want?

- Information concerning:
  - Intelligence Operations
  - Technology
  - R & D
  - Command Strength/Mission/Readiness
  - System Capabilities
  - Security Procedures/Measures
  - Economic/Trade Info

COLLECTION GOALS

"Foreign collectors do not distinguish between military or civilian technology, proprietary information, or traditional secrets…they simply collect what they find to be of value."

(ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 1998)

What Specific Technologies?

- Information Systems
- Aeronautics
- Sensors & Lasers
- Armaments & Energetic Materials
- Electronics
- Marine Systems
- Space Systems
- Materials
- Biomedical

Why Technology?

- Espionage is cheaper/easier than developing your own technology
- Economic as well as Military improvement

"In military and political matters France and the U.S. are allied, we are friends. But in technical and economic matters we are competitors…we are not allied."

Francois Stone Merion/1996

Directorate of External Security (DGSE), France

How Do They Collect?

- Open Source
- HUMINT
- SIGINT
- IMINT

Typical Espionage Collection Techniques?

- Unsolicited Information Requests
  - Internet
- Foreign Employees or "Visitors" at Cleared Facilities
- False Flag
- "Joint Ventures" or Company "Buy Outs"
- Recruit Former Cleared Employees
  - Be a "Consultant"
- Convention/Seminar Attendees

Who is targeted?

- Those with knowledge, placement, & access
- Foreign Travel and Relatives
- Persons with commonalties: Ideological, Religious, Ethnic, Social, etc…
- Individuals with vulnerabilities, weaknesses, needs

Exploitable Weaknesses

- Illegal Activities
- Substance Abuse
- Disgruntlement
- Ego
- Foreign Relatives
- Financial Problems
  - FISS could use above if you do not cooperate
    - "What if I've made a mistake?"

How Does FISS Recruit?

- Spot and Assess
- Collect Bio Data (ID Weaknesses, etc.)
- Evaluate/Assess Recruitability
- Approach/Pitch (Ideology,False Flag, Money)
- Volunteer

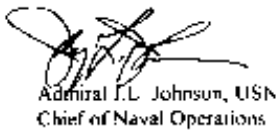
"Where observation is concerned, chance favors only the prepared mind."

Louis Pasteur

07Dec1854

Ask Yourself . . .

- Do documents or Internet info reveal too much or inappropriate information about me, my family or my job?
- Do I have personal information that could be used
  - To compromise a work product or process?
  - As blackmail?
  - To embarrass me?
  - To steal my identity?



Mandatory Reporting

PER DODINST 5240.6 OF 10J UL96/CI AWARENESS AND BRIEFING PROGRAM SECNAVINST 3875.1A

- UNOFFICIAL CONTACTS WITH OFFICIAL(S) OF A FOREIGN DIPLOMATIC ESTABLISHMENT
- REQUESTS FOR UNAUTHORIZED ACCESS TO CLASSIFIED AND/OR CONTROLLED INFORMATION
- SUSPECTED FOREIGN INTELLIGENCE AND SECURITY SERVICES CONTACTS OR TARGETING

Mandatory Reporting

- COMPROMISE, OR INTENT TO COMPROMISE CLASSIFIED / CONTROLLED INFORMATION

- ANOMOLIES WHICH CAN BE DESCRIBED AS FOREIGN POWER ACTIVITY OR KNOWLEDGE INCONSISTENT WITH EXPECTED NORM

Espionage Indicators

- Undue Affluence
- Unexplained Irregular Work Hours
- Attempts to obtain info with no Need to Know
- Unauthorized Removal of Classified Info
- Unreported Foreign Contacts
- Significant Unofficial/Unreported Travel

Espionage is occurring right now!

What if You are Approached?

- Non-Committal
- Observant
- No discussion with others
- Report to NCIS

THREAT

- The Espionage and Terrorist Threats exist more than ever
- These activities affect everyone
- Reporting suspicious activities is more important than ever
- You are our Eyes and Ears
- KNOW HOW TO REPORT!

NAVAL CRIMINAL INVESTIGATION SERVICE
WASHINGTON FIELD OFFICE
(202) 433-3858

HQMC SECURITY OFFICE
(703) 614-2320

THIS CONCLUDES THE CE BRIEF

TO SEND AN EMAIL CONFIRMING THAT YOU HAVE COMPLETED YOUR ANNUAL TRAINING REQUIREMENT BY VIEWING THIS BRIEF ELECTRONICALLY, CLICK THE LINK BELOW:

SEND CONFIRMATION E-MAIL

TO SEND AN E-MAIL TO THE HQMC SECURITY MANAGER WITH QUESTIONS ABOUT THIS BRIEF, CLICK THE LINK BELOW:

SEND E-MAIL WITH QUESTIONS